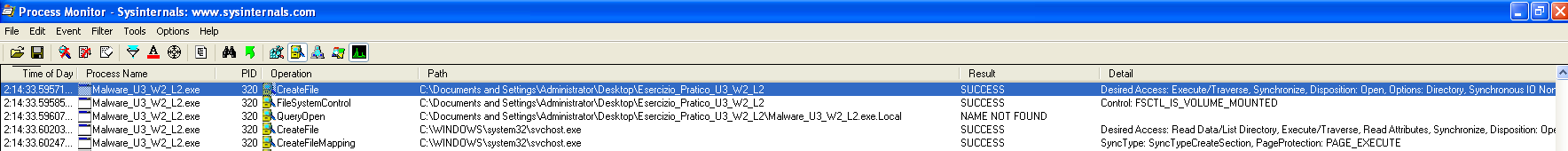
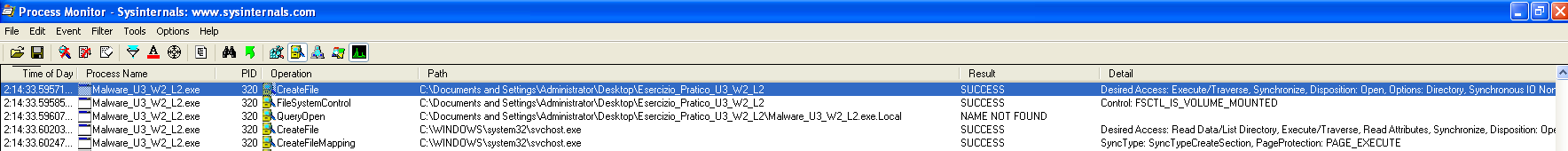
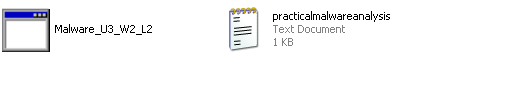
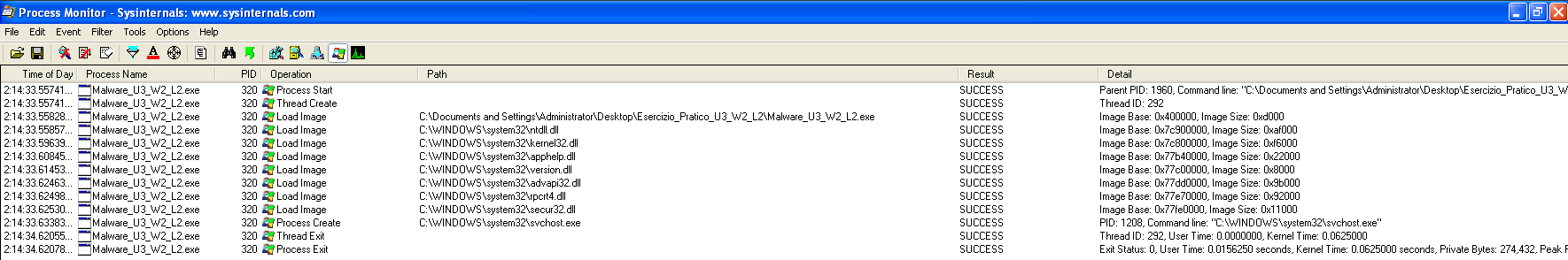
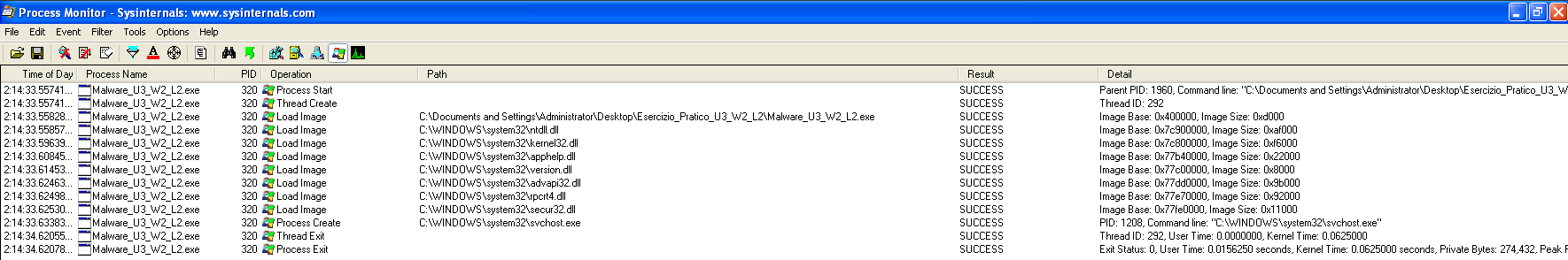
**ANALISI STATICA DINAMICA**

**Traccia**  
Con riferimento al file eseguibile contenuto nella cartella «Esercizio\_Pratico\_U3\_W2\_L2» presente sul desktop della vostra macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti quesiti:  
1) Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon) oppure se ci sono problemi multimon: https://www.resplendence.com/multimon--<https://multimon.it.uptodown.com/windows/download/23982> versione 2.5 per XP.  
2) Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor .  
3) Modifiche del registro dopo il malware(le differenze).  
4) Provare a profilare il malware in base alla correlazione tra «operation» e Path.  
  
**Teoria**  
**SVCHost.exe**: un processo di sistema generico di Windows, che può ospitare uno o più servizi del sistema operativo, molto spesso essenziali al funzionamento del computer. In passato, SVCHost.exe è stato un nome spesso sfruttato da autori di malware per realizzare dei file malevoli in grado di “nascondersi” all’interno dei numerosi servizi di Windows per agire più o meno indisturbati. Per prevenire i problemi è possibile ricorrere a software di protezione, magari verificando prima cos'è e come funziona un software antivirus. Vediamo ora cos’è e a cosa serve SVCHost.exe, per poi cercare di capire come fermare eventuali minacce informatiche che sfruttano questo particolare servizio Windows. A cosa serve SVCHost.exe SVCHost.exe viene definito, da Microsoft, come un nome generico che viene assegnato ad un processo Host di Windows. Si tratta, quindi, di una parte integrante del sistema operativo ed è necessario al corretto funzionamento di vari aspetti del sistema operativo di Microsoft. Il ruolo di SVCHost.exe è chiaro. Questo processo, infatti, funge da shell per il caricamento di file DLL (Dynamic-link library) che comprendono librerie software che vengono caricate, in modo dinamico, in fase di esecuzione invece di essere collegate staticamente ad un file eseguibile in fase di compilazione. SVCHost.exe nasce, quindi, con l’obiettivo di utilizzare i file DLL che integrano il codice necessario al corretto funzionamento del sistema operativo. I processi Host di Windows sono un componente chiave dell’intera architettura software del sistema operativo e si occupano di avviare le librerie software che consentono agli utenti (e alle varie applicazioni installate nel proprio dispositivo) di attivare e utilizzare le varie funzionalità di Windows.  
  
**Soluzione**

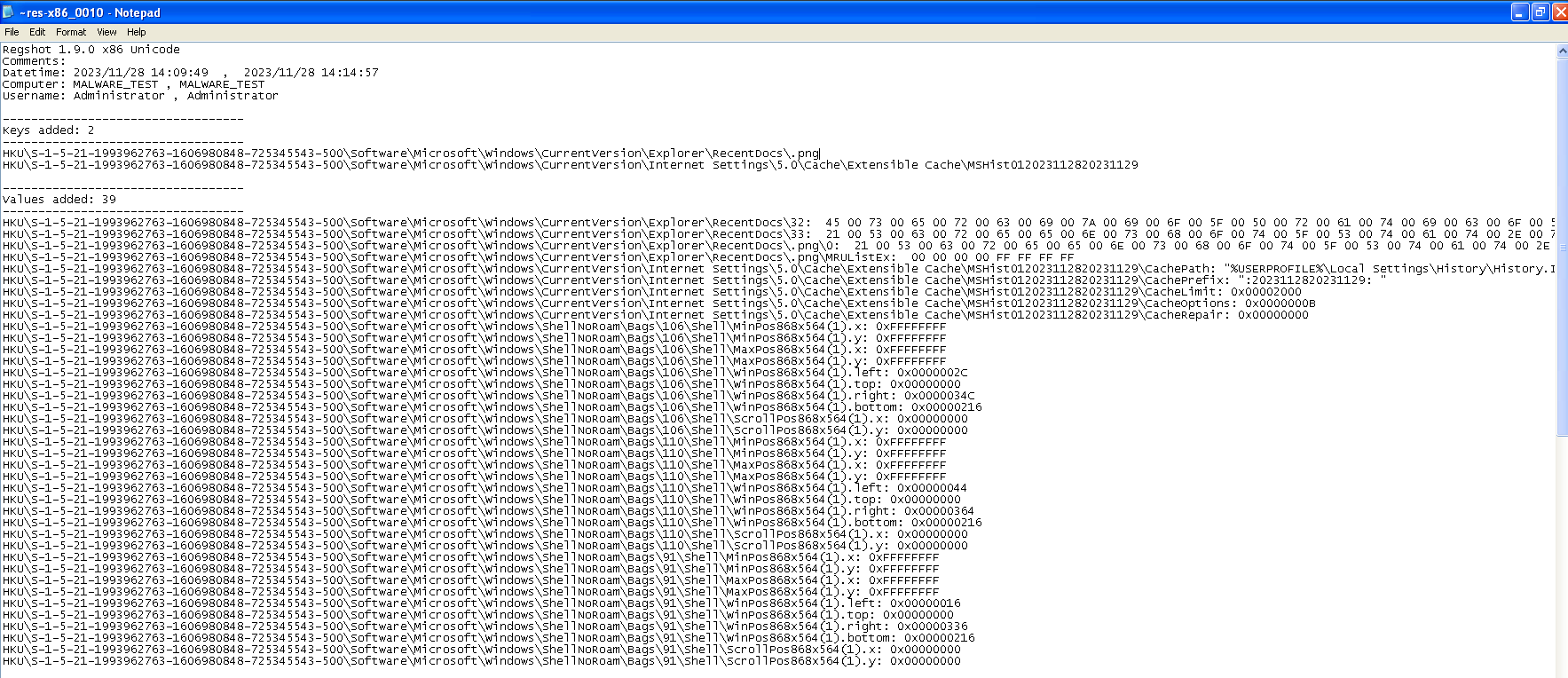
1) Iniziamo aprendo RegShot, ProcessoMonitor e ProcessExplorer.  
Facciamo un primo shot con RegShot ed eseguiamo il malware.

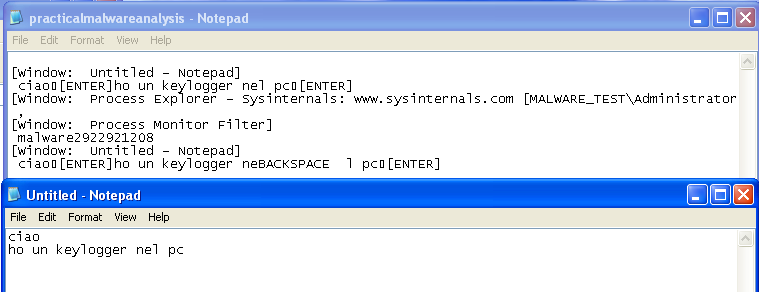
Possiamo notare come il Malware sia andato a creare un file (CreateFile) nel percorso stesso del malware.  
Andiamo a controllare e troviamo un file di testo.

  
2) Andando ad esaminare i processi tramite Process Monitor ed il filtro “ProcessName Contains Malware\_U3\_W2\_L2.exe”.



  
  
  
Troviamo diverse operazioni eseguite dal malware. Possiamo vedere come molte operazioni siano richiami a delle funzioni di sistema. Ne notiamo una in particolare ovvero “Process Create” con PID: 1208. Si ricollega al seguente:

3) Screen - Compare di RegShot

  
4) Profilazione  
Possiamo notare che nel file di testo creato, troviamo buona parte di quello che facciamo sul nostro dispositivo, motivo per cui possiamo dedurre che il malware sia un keylogger.